

APPENDIX D

408250" 55020005

A MIB For Video Server System Management

David Robinson

Video Interactive Information Services Group (VIISG)

Digital Equipment Corp., Imperial Way, Reading, Berkshire, UK

Don Hooper

Video Interactive Information Services Group (VIISG)

Digital Equipment Corp., Shrewsbury, MA 01545, USA

Abstract - A video server system provides many different types of interactive video services including: video on demand, home shopping, interactive games, etc. Both the use of the interactive video services and the video server itself need managing. This ranges from configuring the system, handling and logging faults, through monitoring the performance, etc. This paper describes how to structure the Management Information Base (MIB) for managing DAVIC compliant video server systems. It is described in terms of the management protocol developed by Internet Engineering Task Force (IETF) known as Simple Network Management Protocol (SNMP).

1. INTRODUCTION

The term *Network Management* is often used to describe management of more than just networks. Indeed, many of the techniques and tools developed for monitoring and controlling a network are equally suited to management of distributed systems. This is the case with video server systems. This paper describes how the network management concepts and tools developed by the IETF (Internet Engineering Task Force) under the banner of SNMP (Simple Network Management Protocol) can be applied to video servers.

This section describes the general concepts of management and introduces some of the features of SNMP. Section II covers some of the key areas for management of video server systems. It then describes how SNMP MIBs can be defined to instrument these areas. This is based on the draft MIBs being defined by the Digital Audio Visual Council (DAVIC). In section III, we consider some of the security implications of using SNMP and identify some measures we can take.

A. Network Management Concepts

Aspects of Management

It is traditional to divide network and system management into 5 aspects representing the main management tasks: Fault, Configuration, Accounting, Performance, and Security.

- **Fault Management:** It encompasses fault detection, isolation, and the correction of abnormal behaviour of the system. The fault may be permanent or transient. Faults may be detected by events or by polling. A single fault may manifest itself as several events. Hence, fault management must be capable of correlating several events to determine the true fault.
- **Configuration Management:** This aspect of management is concerned with the configuration of the system. It involves starting and stopping components of the system, changing the parameters used to control the system, and changing the software and / or hardware.
- **Accounting Management:** It determines the use an individual user makes of the system with the aim of informing the user of costs incurred or resources used. It is also involved with setting of accounting limits and tariff schedules associated with particular resources.
- **Performance Management:** It is concerned with monitoring the behaviour of resources. It is used for provisioning planning and preventative maintenance.
- **Security Management:** It is used to implement the security policies. These include control of authentication keys, user access permissions and confidentiality.

Levels of Management

Another way of looking at network and system management is to divide it into levels spanning the 5 functional aspects. Each level represents a different level of detail. There is a part of each aspect of management in each level.

- **Element Management:** This is the lowest or most detailed level of management. It is concerned with the monitoring and control of individual components of a system. In interactive video systems, this corresponds to monitoring and control of the individual hosts in a video server system and of the other networking equipment.

- **System Management:** This level puts together the information from separate elements to provide a complete view of some part of the system. This gives integrated management of the elements within the subsystem.
- **Service Management:** Service management is concerned with management of the services provided by the system as seen by the users. In video interactive systems, this includes monitoring and control of the video on demand service, home shopping service, interactive games service, etc.
- **Business Management:** Business management is concerned with setting business policy for the system and receiving summary information concerning the operation of the system and the services provided.

The focus of this paper is on element management. That is, getting the raw data and providing low level control upon which the other levels of management can be based.

B. Use of SNMP for Element Management

For element management, we need to be able to monitor and set individual components within the video server system. There are two aspects to this. Firstly is the specification of the components to be managed. These are usually referred to as *managed objects*. A collection of managed objects is termed *management information base* or MIB. Secondly, we need a protocol to read and write these managed objects. There are two standard element management protocols: ISO's Common Management Information Protocol (CMIP [1]) and IETF's SNMP [3].

SNMP is preferred over CMIP for several reasons including:

1. **Widely implemented:** SNMP is available on most operating systems.
2. **Cheap to implement:** There are several tools which make it easy to implement video server specific SNMP MIBs.
3. **Widely supported:** Most Network Management Stations support SNMP.
4. **Functionally sufficient:** Provides most of the functionality required - although filtering of data at source would be preferred.
5. **Standard MIBs:** these cover much of the basic monitoring and control of the video server hardware. There are several widely used tools which use these MIB objects to report management information.

The main objections to SNMP are its weak security and inability to return multiple entries from a table or to filter returned values. These objections are resolved in SNMPv2

[9] which is currently going through the IETF standards process.

SNMP only supports operations to GET and SET (read and write) managed objects. All changes in state occur by side effect of setting managed object(s) to specific values. There are no CREATE, DELETE, ENABLE, nor DISABLE operations.

SNMP also supports an asynchronous operation which can be raised by an agent called a TRAP. This is used to signal exceptional events or alarms. The TRAP PDU is sent to multiple destinations. It is unacknowledged to keep the agent simple.

In summary, SNMP provides the basic functionality for element management. Using the SNMP Structure of Management Information (SMI) notation, it is possible to define all the elements which need monitoring and through which control is achieved. The next section describes how to apply SNMP to video server systems.

II. VIDEO SERVER MIB STRUCTURE

A. Motivation for Management of Video Server System

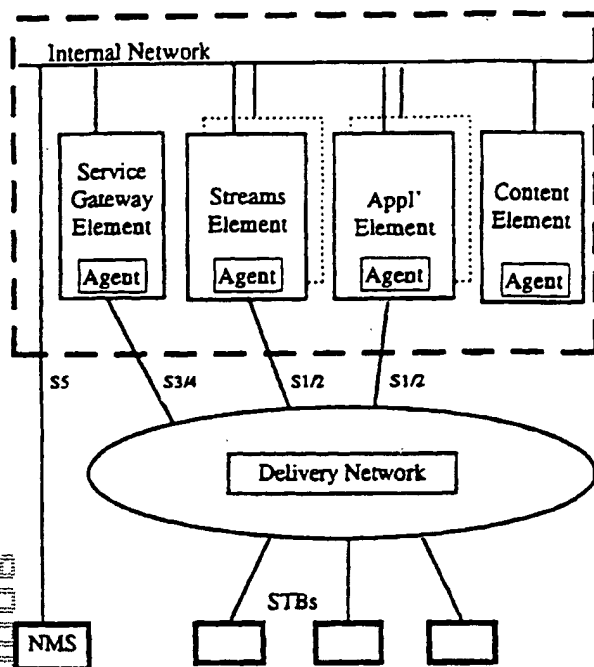
Video server systems, as part of the overall video interactive systems, need managing. We will look at three particular users of management: *customer care center*, *field service*, and *business management*. They have different needs of management information and control.

Customer Care Center needs knowledge of the current state of the video server system. For example, the operators need to know which users have been affected by a failure within a video server system. Operators need also to be able to register new users and change the rights of existing users in response to user requests.

Field Service need to identify faults in the hardware platform of the video server and failures in the software. They are also interested in trends in recoverable failures such as packet loss or recoverable disk failures. These trends are used for preventative maintenance. They need to be able to change the configuration of the video server system, for example, to install a new version of the software or alter some operational parameter.

Business Management is interested in usage trends for capacity planning and tuning of business policy. Also need actual usage data for billing purposes. They need to be able to initiate the change in content of the video server and to alter the tariffs for usage.

B. DAVIC Server Architecture



The Digital Audio Visual Council (DAVIC) server architecture consists of several logical *elements*: service gateway, stream, application, and content. The service gateway mediates all user access to the video server. It maintains the user profiles and can authenticate a user request for a session. It also supports downloading client applications to the set top boxes (STBs). Stream and application elements are allocated to a session based on the requested services. The stream elements are launched to support VOD (Video On Demand), NVOD (Near VOD) and broadcast applications. The content element is used to manage the video content of the video server. It is the way new content is loaded and moved internally to the video server.

The elements are linked to set top boxes via interfaces into the delivery network. There is a slow speed connection used to establish sessions. This is via the Service Gateway element. Also, there are interfaces into the high speed delivery network for communicating MPEG streams. The interfaces used by the STBs are referred as S3, S4 (for control) and S1 and S2 (for user requests and video stream). This follows the distinction in DSM-CC [11] of separate interfaces and protocols for user-to-network (U-N) and User-to-user (U-U). There is a separate interface used for management. This is designated S5.

The S5 interface allows a network management station (NMS) to monitor and control a video server system. Each element has to support the relevant part of the S5 interface. This allows monitoring and control of the elements. S5 uses SNMP as the access protocol. Network management stations may access S5 via the delivery network or some other private network. It is connected to the internal communications network to allow access to the network management agents of the elements.

The S5 interface is also used to monitor and control the underlying video server framework - the hardware and middleware - which supports the video server elements. For example, this will allow monitoring of the computer nodes, disk activity and network traffic on the physical network interfaces. It can also be used for changing the configuration of the video server system. This monitoring and control of the framework will use a combination of standard MIBs and vendor specific MIBs.

Note, this does not mean that each element has to have its own SNMP agent executing on the same node as the element itself. Rather, proxy agents executing on another node can be used if desired.

C. Monitoring points for Video Server Systems

This section identifies some of the key monitoring and control points for management of a video server system.

- **Communication Interfaces:** A video server system will have several physical interfaces into the delivery network. These are to support the S1, S2, S3 and S4 services. In addition, there may be other interfaces for S5 access. These are monitored to detect loading and error rates, etc. Much of the monitoring can be performed using existing standard MIBs.
- **Video Server Framework:** The hardware and middleware providing a video server system needs to be monitored for faults and performance. Management is also used to control the video server. Some of the monitoring can be performed using standard MIBs but much will be video server specific. Management is also used to configure the supporting framework.
- **Service Gateway Element:** This element is used to process all end user requests for a service. It contains the user profiles, knowledge of resources in use, list of active sessions, etc. Network management can be used to query the above information and potentially used for control. For example, it could be used to terminate a session or stream.

- **Streams Element:** Management needs to be able to query the active streams and potentially to terminate a stream. It should be possible to relate a stream with the end user and the local access point into the delivery network.
- **Application Elements:** there are many types of applications. Each type will have a specific MIB. However, there are several common features of all applications, such as which users are using the application, which interfaces into the delivery network are being used, etc. This application information can be included in a common application MIB.
- **Content Element:** This element provides the means to monitor and control the content of the video server.

D. MIB Structure

Each element type provides a distinct set of functions. Therefore, we can structure the MIBs to represent this division of functionality. Each element type has its own set of managed objects. These are provided by separate MIB definitions - one per element type. This division permits the introduction of new element types without having to modify existing MIBs, e.g. a new application. Currently, DAVIC has draft specification for the following MIBs [10]:

- **Service Gateway MIB:** This MIB has tables for *sessions*, *user profiles*, and *application load*. The *sessionTable* lists the active sessions with this video server system. It identifies the end user associated with a session and any associated streams and/or application elements. The User profile and application load tables contain information used when initiating a session.
- **Stream Element MIB:** This lists the streams active with this element. It identifies the content being played out, the current state (play, fast forward, pause, etc.) and position. It also identifies the end user and the local interface through which the stream is being played out. There are also counters for the total number of streams played, aborted, and rejected.
- **Application MIB:** This is a generic MIB for all applications other than Video On Demand. It identifies the end user of the application and the local interface being used by the stream.
- **Content MIB:** There are several tables which identify the content of the video server system. This includes identifying who provides the content and the content

type as well as specific information about the content itself.

SNMP was deliberately kept simple. There are no constructed data types, only simple objects (INTEGER, Counter, Gauge, OCTET STRING, Display String, etc.) A MIB definition consists of managed objects of these simple types. In addition, SNMP supports the notion of tables. Each row in the table consists of one or more managed objects, the number and type being defined in the MIB. There can be an arbitrary number of rows in the table. Each row is uniquely identified by an index.

To illustrate the approach taken in the draft DAVIC MIBs, we will discuss the Streams Element MIB and the Sessions Group in the Service Gateway MIB. Only sufficient fragments of the MIBs are included for the discussion.

Streams Element MIB

The streams Element MIB contains several counters, some TRAPs and the *streamTable*. The counters record the number of streams initiated, rejected and aborted with this streams element. The TRAPs are used to report on exceptional changes in state of a stream such as rejections, aborted streams, and communications problems.

The definition of the *streamTable* is as follows:

```
streamEntry      OBJECT-TYPE
    SYNTAX        StreamEntry
    ACCESS        non-accessible
    STATUS        mandatory
    DESCRIPTION   "Table of active streams with this streams element"
    INDEX ( streamIndex,
            streamSessionId,
            streamIndex )
 ::= { streamTable 1 }

StreamEntry ::= SEQUENCE
{
    streamIndex      INTEGER,
    streamIndex      INTEGER,
    streamSessionId  INTEGER,
    streamType       INTEGER,
    streamBandwidth  INTEGER,
    streamDirection  INTEGER,
    streamPosition   INTEGER,
    streamState      INTEGER,
    streamRowStatus  RowStatus
}
```

Each stream in a streams element will have its own entry in the streams table. The meaning of each field is:

- *streamIndex* - a unique identifier for this stream entry.
- *streamIfIndex* - index into the standard MIB-II *ifTable*. This identifies the local network interface into the delivery network being used by this stream.
- *streamSessionId* - index into the *sessionTable* in the Session Element MIB.
- *streamType* - MPEG-2 or H-261 stream
- *streamBandwidth* - measured in Mbps
- *streamDirection* - direction for stream relative to set top box
- *streamPosition* - measured in second from the start.
- *streamState* - state of the stream, Play, Fwd, Rwd, Pause.
- *streamRowStatus* - used to control the entry including deleting the stream.

Session Service Group

This group is part of the Server Gateway Element MIB. It records the current sessions and TRAPs for unusual events related to sessions. There is also a *sessionTable* which records the currently active sessions.

```

SessionEntry OBJECT-TYPE
    SYNTAX      SessionEntry
    ACCESS      non-accessible
    STATUS      mandatory
    DESCRIPTION
        "list of current active sessions"
    INDEX (sessionIndex)
SessionEntry ::= SEQUENCE
    ::= (sessionTable 1)
StreamEntry ::= SEQUENCE
    (
        sessionIndex      INTEGER,
        sessionSessionId  OCTET STRING (SIZE(6)),
        sessionStartTime  DateAndTime,
        sessionEndTime    DateAndTime,
        sessionStreams     IpAddress,
        sessionApplications IpAddress,
        sessionStatus      INTEGER,
        sessionRowStatus   RowStatus
    )

```

- *sessionIndex* - is the unique reference of the session
- *sessionSessionId* - identifier of this session used in protocols to and from STBs.
- *sessionStartTime* - time this session started or is scheduled to start
- *sessionEndTime* - time this session is due to end
- *sessionStreams* - identifier of the stream supporting this session, if any.
- *sessionApplications* - identifier of the application supporting this session, if any.
- *sessionStatus* - state of the session.

- *sessionRowStatus* - used to control the session entry including delete the session.

Note: the identity of the user of this session is not included in the *sessionTable*. Rather, there is another table of clients to the video server. Each entry contains a field *sessionIndex*. Using this field, it is possible to relate users with their sessions.

Where possible, standard MIBs should be used. IETF have already standardized several communications oriented MIBs, the most important of which is MIB-II (RFC1213[4]). This is a generic MIB for monitoring the state of communication interfaces. The basic table in MIB-II is *ifTable*. There is an entry in this table for each interface in the system. This has counters for the number of octets / packets sent and received and the number of errors as well as the type of the interface and its current state.

Rather than duplicating this information, the *streamTable* and *applicationTable* reference the *ifTable*. For example, the *streamsIfIndex* is a reference into the *ifTable*.

There are other MIBs which are interface type specific. They have managed objects for a particular interface type such as FDDI (RFC1512 [5]), and ATM (RFC1695 [8]). These are also keyed off *ifIndex*. Hence, it is possible to browse through management information starting with a stream into the *ifTable* to get general information about the interface and onto a MIB for a specific network type. This is useful in fault finding and to correlate alarms. For example, if a particular interface fails, several streams are likely to be affected. For each one, a *streamCommunicationTrap* will be generated. This TRAP includes the *ifIndex* of the affected interface.

In addition to communications oriented MIBs, there are several MIBs designed for monitoring 'hosts'. For example, the HOST MIB (RFC1514 [6]) contains several managed objects and tables for monitoring host resources (disk, processor, memory etc.). Also, the Network Services Monitoring MIB (RFC1565 [7]) defines a standard way of identifying the applications running on a node.

There are several network management tools available which interrogate these standard MIBs. These tools may be for presenting a graphical view of system loading or for trend analysis, etc. By using the standard MIBs, where appropriate, in video server systems, these tools are available for monitoring and control.

The Elements model for Video Server Systems lends itself to a distributed implementation. To permit loosely coupled distributed implementations, we have to support distribution

of the MIBs. For example, to get the desired performance, a vendor may choose to implement the service gateway as well as the streams elements on one or more nodes.

Each node supporting a streams element will have its own *streamTable*. This will record only those streams being handled by that streams element. A node providing the service gateway element will support the Service Gateway MIB. This MIB contains the *sessionTable*.

The basic SNMP model assumes all the MIBs run on the same node. For example, The link between one table and another is just the index into the other table. For a potentially distributed implementation, this is not sufficient information. Therefore, we use the IP address of the agent supporting the referenced MIB.

Hence, in the DAVIC MIB, the *sessionTable* identifies the stream associated with a session by the *sessionStreams* field. This is the IP address of the SNMP agent supporting the corresponding *streamTable*. It is not necessary to include the *streamIndex*, as the *streamTable* is indexed by with the *sessionIndex*. Thus, the following sequence of SNMP requests can be used to trace a session entry to a stream. Lookup the *sessionStreams* field in the *sessionTable* to determine the IP address of the agent supporting the relevant *streamTable*. Then, using the *sessionIndex* value as the index, query the relevant SNMP agent to read the entry from the *streamTable*.

All nodes, apart from the service gateway nodes, have a managed object which identifies the IP address of the service gateway node. An agent representing a Service Gateway maintains a table of other elements, the *elementsTable* (see below). Using this table, it is possible to discover the SNMP agents responsible for the other elements.

```

elementEntry      OBJECT-TYPE
    SYNTAX          ElementsEntry
    ACCESS          not-accessible
    STATUS          optional
    DESCRIPTION
        "The list of SNMP agents of this video server"
    INDEX (elementsIndex)
::= { elementsTable 1 }

```

ElementsEntry ::= SEQUENCE

```

(
    elementIndex      INTEGER,
    elementName       DisplayString,
    elementType       DisplayString,
    elementIpAddress  IpAddress,
    elementStatus     INTEGER,
    elementRowStatus  RowStatus
)

```

- *elementsIndex* - unique identifier of this entry
- *elementName* - name of the node supporting the element
- *elementType* - type of the element
- *elementIpAddress* - address of the node supporting the element
- *elementStatus* - last known state of the element
- *elementRowStatus* - indicates the state of the entry.

The *ifTable*, and other standard MIBs, are assumed to be local. Therefore, it is not necessary to use IP address when referencing these tables.

Note, the draft DAVIC MIBs permit a single agent implementation. The IP addresses to other agents will be that of the node itself. The *elementsTable* need not be provided in this case.

In addition to the DAVIC standard MIBs, vendors can provide their own MIB. This will enable monitoring and controlling their specific implementations. This is common practice in SNMP management. The standard MIBs define managed objects for general monitoring and control. The vendor specific MIB may often be needed for specific management.

E. System and Service Management using MIBs

In this section, we briefly discuss how the DAVIC MIBs can be used for system and service management.

We can start and stop individual elements for basic configuration management. TRAPs generated by individual elements can be used to initial recovery action where necessary for fault management. The *elementsTable* in the service gateway element is useful to determine which nodes are supporting agents of this video server system.

The *streamTable* and *applicationTable* enable us to monitor the service being provided by the video server system. It can be used as the basis for billing as well as customer care should there be a failure. It can also be used for management of the content if desired.

III. SECURITY CONSIDERATIONS

It is necessary to protect network management access to the Video Server System. The S5 interface uses well known protocols (SNMP over UDP) and the standard MIBs are public. Hence, we need security steps to prevent unauthorized changes or degraded performance. There are several options available.

A. Physical Separation

Provide a separate network for S5 interface from that used by the set top boxes. This ensures that only permitted NMSs can access the S5 interface. This is not always possible or desirable. For example, you may wish to allow remote access to field server engineers to diagnose a fault.

B. Screen or Route Filtering

Screen is an application which filters access based on source and destination IP address and port number. SNMP requests are carried on UDP and sent to the SNMP request port number 161. We know the set of network management stations which are authorized to access the video server MIBs. Hence, we can filter out all UDP messages to port 161 unless it comes from a recognized and authorized network management station. However, IP addresses can be faked.

C. Community Name

SNMP has the notion of communities. An SNMP administrator can limit access to particular MIB variables on a community by community basis. Each request contains a community name. The video server administrator will validate the use of this community name against the source address. If that community is not authorized from that source address, then the agent refuses the request and issues an *authenticationFailure* TRAP. As some objects may be considered more sensitive than others, then we can use different community names. For example, it is common to use the community name public for reading the *system* group in MIB-II.

D. SNMPv2 Security Features

The IETF recognize that one of the main shortcomings of the first version of SNMP was its lack of security. This is being addressed in SNMPv2. When SNMPv2 stabilizes, then its security features should be used.

IV. SUMMARY

SNMP provides a suitable basis for element management of a video server system. It is widely deployed for managing data networks and there are already many tools and network management stations which could be used to manage a video server system and the entire video interactive system.

This paper has shown the approach being taken in DAVIC for managing the elements of a video server system. In particular, it defines how loosely coupled distributed implementations can be handled. The MIB specification effort has just started and much more work is needed.

V. ACKNOWLEDGMENTS

The authors wish to thank Greg Johnson and Lee Arnold for the implementation experience of the DAVIC style MIBs. Also, Suban Krishnamoorthy provided much valuable feedback and publication assistance on this paper. This project work has been carried out at Shrewsbury, Mass, USA.

VI. REFERENCES

- [1] ISO/IEC 9596:1989 "Information technology - Open Systems Interconnect - Common Management Information Protocol Specification", International Standards Organisation, 1989.
- [2] ISO/IEC 10165-4:1992, "Information Technology - Open Systems Interconnect - Structure of Management Information - Guidelines for the Definition of Managed Objects", International Standards Organisation, 1992.
- [3] M. Rose, K. McCloghrie, "Structure and Identification of Management Information", STD-16, RFC1155, Performance Systems International, Hughes LAN systems, May 1990.
- [4] M. Rose K. McCloghrie, Editors "Management Information Base for Network Management of TCP/IP Based Internets", STD-17, RFC1213, Performance Systems International, March 1991.
- [5] J. Case, A. Rijsinghani, "FDDI Management information Base", RFC1512, SNMP Research Inc., Sept 1993.
- [6] P. Grillo, S. Waldbusser, "Host Resources MIB", RFC 1514, Intel Corporation, September 1993.
- [7] S. Kille, N. Freed, "Network Services Monitoring MIB", RFC 1565, ISODE Consortium, Jan 1994.
- [8] M. Ahmed, K. Tesink, "Definition of Managed Objects for ATM Management Version 8.0 using SMlv2", RFC1695, Bell Communications Research, Aug 1994.
- [9] J. Case, K. McCloghrie, S. Waldbusser, "Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)", RFC1442, SNMPResearch Inc. April 1993.
- [10] D. Robinson, "Video Server Provider Instance MIB", DAVIC/TC/SER/95/02, The Digital Audio-Visual Council, March 1995.
- [11] MPEG-2 DSM-CC Subgroup, "ISO/IEC 13818-6: MPEG-2 Digital Storage Media Command and Control 2nd Working Draft", ISO/IEC JTC1/SC29/WG11 N0926, March 1995.

Author

Robinson D. Hooper D.

Institution

Digital Equipment Corp., Reading, UK.

Title

A MIB for video server system management.

Source

Proceedings of the 2nd International Workshop on Community **Networking Integrated Multimedia Services in the Home** (Cat. No.TH8097). IEEE. 1995, pp.109-15. New York, NY, USA.

Conference Information

Proceedings of the Second International Workshop on Community **Networking Integrated Multimedia Services to the Home**. Princeton, NJ, USA. IEEE Commun. Soc. ACM SIGCOMM. 20-22 June 1995.

Abstract

A video server system provides many different types of interactive video services including: video on demand, home shopping, interactive games, etc. Both the use of the interactive video services and the video server itself need managing. This ranges from configuring the system, handling and logging faults, through monitoring the performance, etc. This paper describes how to structure the management information base (MIB) for managing DAVIC compliant video server systems. It is described in terms of the management protocol developed by Internet Engineering Task Force (IETF) known as the Simple **Network Management Protocol (SNMP)**. (11 References).

102259-052004